IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

ASPIRE HEALTH, INC.,	)	
Plaintiff,	)	**Civil Action No. _____**
vs.	)	**Jury Demanded**
JOHN DOE I, and individual,	)	
Defendant.	)	

COMPLAINT

Pursuant to Rule 3 of the Federal Rules of Civil Procedure, Plaintiff Aspire Health, Inc., complaining of Defendant, alleges and says as follows:

PARTIES

1. Plaintiff Aspire Health, Inc. ("Aspire") is a corporation organized and existing under the laws of the State of Delaware and has its principal place of business in Nashville, Tennessee.

2. Defendant John Doe I is an individual of unknown residence and citizenship. Aspire does not know John Doe I's identity or location at this time. Aspire will amend its complaint to name John Doe I when his or her identity is learned.

JURISDICTION AND VENUE

3. This Court has federal question jurisdiction over this action under 28 U.S.C. § 1331 because this action alleges violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 and Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et. seq*.

4. Venue is proper in this District under 28 U.S.C. § 1391(b)(2). Depending on the residence of defendant, venue may be proper under 28 U.S.C. § 1391(b)(1) or (3) as well.

FACTS AND BACKGROUND

5. Aspire is a health care company that specializes in arranging for palliative medical care for patients facing symptoms, pain, and stress of serious illnesses.

6. Aspire uses a Microsoft Office 365 e-mail system and maintains the e-mail system on protected computers. Within the e-mail system, Aspire employees maintain confidential and proprietary communications, information, and files.

7. Aspire's e-mail system on its protected computers is secured by Aspire and access requires credentials unique to each Aspire employee. No one external to Aspire is authorized to access the e-mail system on the protected computers.

8. On September 5, 2018, Aspire discovered that an Aspire employee was the victim of a phishing attack e-mail initiated by John Doe I and originating from a website registered to an IP address located in Eastern Europe (the "Phishing Attack"). Google is the registrar of the website.

9. As a result of the Phishing Attack email, John Doe I acquired security credentials unique to the Aspire employee and gained unauthorized access to Aspire's e-mail system on a protected computer. Upon accessing the e-mail system on the protected computer, John Doe I created a rule within the Microsoft Office 365 system that forwarded 124 e-mails to an external e-mail account maintained by John Doe I of which Google is the provider.

10. The e-mails extracted from the protected computer contain confidential and proprietary information and files, and a portion of the e-mails contain protected health information.

CLAIM FOR RELIEF
(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

11. Aspire hereby incorporates by reference and re-alleges the preceding paragraphs of this Complaint.

12. Aspire's e-mail system is secured and stored on Aspire protected computers, which are connected to the internet and used in interstate commerce.

13. John Doe I intentionally accessed Aspire's protected computers without authorization through the Phishing Attack and extracted Aspire's confidential and proprietary electronically stored information.

14. John Doe I's access and extraction of Aspire's electronically stored information has economically harmed Aspire in an amount that exceeds $5,000 in a 1-year period, including, among other things, the incurred costs of responding to and investigating John Doe I's illegal actions.

CLAIM FOR RELIEF
(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et. seq)*

15. Aspire hereby incorporates by reference and re-alleges the preceding paragraphs of this Complaint.

16. John Doe I has violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701 *et seq.*, by (a) intentionally accessing without authorization Aspire's e-mail system; (b) extracting and obtaining Aspire's electronic communications while such communications were in electronic storage by implementing a forwarding rule in Aspire's e-mail system; and (c) disclosing such electronic communications by sending the intercepted electronic communications to an e-mail account outside of Aspire.

17. Aspire has been irreparably damaged by John Doe I's violations of Title II of the Electronic Communications Privacy Act, and is entitled to damages, punitive damages injunctive relief, and attorneys' fees and costs pursuant to 18 U.S.C. § 2707.

JURY DEMAND

18. Pursuant to Federal Rule of Civil Procedure 38(b), plaintiff demands a trial by jury as to all issues so triable in this action.

PRAYER FOR RELIEF

WHEREFORE, Aspire prays for the following relief:

1. For injunctive relief, as follows: An order barring defendant from any further acts constituting violations of the Computer Fraud and Abuse Act and Title II of the Electronic Communications Privacy Act, including any attempts to access electronically stored information from Aspire's e-mail system or any attempts to transfer such electronically stored information to any other person or entity, and directing defendant to immediately return to Aspire any electronically stored information described herein;

2. For judgment in favor of plaintiff, and against defendant, for damages in such amounts as may be proven at trial;

3. For punitive damages;

4. For reasonable attorneys' fees; and

5. For such other relief as the Court may deem just and proper.

September 21, 2018

NELSON MULLINS RILEY & SCARBOROUGH, LLP

By: */s/ James A. Haltom*

James A. Haltom (BPR No. 28495)
150 Fourth Avenue, North, Suite 1100
Nashville, TN 37219
Phone: (615) 664-5339
E-Mail: james.haltom@nelsonmullins.com
Attorney for Plaintiff Aspire Health, Inc.